IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Pierre Girard	)	Group Art Unit: 2139
	)	
Application No.: 10/590,214	)	Examiner: A. F. Tabor
	)	
Filed: August 22, 2006	)	Confirmation No.: 6719
	)	
For: METHOD OF PRODUCING A DIGITAL CERTIFICATE, AND AN ASSOCIATED DIGITAL CERTIFICATE	)	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal is from the decision of the Examiner in the Final Office Action mailed May 28, 2008, and Appellant's Notice of Appeal filed November 26, 2008, setting a period for response that extends through February 26, 2009, by a Petition for Extension of Time (one month) filed herewith.

Please charge the $540.00 fee for filing this Appeal Brief to credit card. The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

I. Real Party in Interest

The present application is assigned to Gemplus, now GEMALTO SA. GEMALTO SA is the real party in interest, and Gemplus is the assignee of Application No. 10/590,214.

II. Related Appeals and Interferences

None.

III. Status of Claims

Claims 1-12 were originally filed in this application. Claims 13-20 were added by a Preliminary Amendment filed August 22, 2006. The present status of the claims is as follows:

claims 1-20 are currently pending;

claims 1-20 are rejected under 35 U.S.C. § 112, first paragraph;

claims 1-9 & 13-20 are rejected under 35 U.S.C. § 102(e);

claims 10-12 are rejected under 35 U.S.C. § 103(a); and

claims 1-20 are being appealed.

IV. Status of Amendments

None.

V. Summary of Claimed Subject Matter Recited in Claims 1 & 8

Appellant's specification discloses a method of producing a digital certificate and an associated certificate containing information enabling a third party who receives a signed message to estimate the probability that the sender of the transaction is indeed the authentic proprietor of the private key used for the signature. According to an exemplary embodiment, a certificate authority compiles a data set containing a public key and digital data that identifies the owner of the public key and an associated private key, and subsequently signs

that data set to produce a digital certificate. The digital data also includes data that identifies a device for generating the private key and/or storing the private key on a support and/or signing with the private key. The method can be used, for example, to produce X509-type digital certificates.

The present application contains two (2) independent claims – 1 & 8. A mapping of each of the independent claims to one instance of an exemplary embodiment described in the disclosure is set forth in the following table:

CLAIM 1:	**PUBLISHED SPECIFICATION**
A method of producing a digital certificate in which a certification authority performs the steps of:	P. 2, ¶ 0028
grouping together, in a data set, a public key and digital data comprising data identifying the proprietor of said public key and of an associated private key;	P. 2, ¶ 0028
signing the data set in order to produce a digital certificate; and	P. 2, ¶ 0028
storing the signed data set in a computer-readable storage medium,	P. 2, ¶ 0029
wherein the digital data also comprise data identifying at least one of: means of generating the private key, means of storing the private key on a medium, and means of signing with the private key.	P. 2, ¶¶ 30-38

CLAIM 8	
A digital certificate stored in a computer-readable medium, comprising:	P. 2, ¶ 0053
- a public key;	P. 2, ¶ 0054
- data identifying a proprietor of the public key and of an associated private key; and	P. 2, ¶ 0055
data identifying at least one of means of generating the private key, means of storing the private key on a medium, and means of signature with said private key.	P. 2, ¶ 0056

VI. Grounds of Rejection to be Reviewed on Appeal

(1) Whether claims 1-20 are patentable under 35 U.S.C. § 112, first paragraph;

(2) Whether claims 1-9 & 13-20 are patentable under Section 102(e) over U.S. Patent Application Publication No. 2003/0115457 to Wildish et al. ("Wildish"); and

(3) Whether claims 10-12 are patentable under 35 U.S.C. § 103(a) over *Wildish* in view of U.S. Patent Application Publication No. 2004/0123107 to *Miyazaki et al.* ("*Miyazaki*").

VII. Argument

Rejection of Claims 1-20 Under 35 U.S.C. § 112, First Paragraph.

The first paragraph of 35 U.S.C. § 112 states, "The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same." Furthermore, "[t]he description need *only* describe in detail that which is *new or not conventional*." *See* M.P.E.P. § 2163(II)(3)(a), *citing Hybritech v. Monoclonal Antibodies*, 802 F.2d at 1384, 231 USPQ at 94; *Fonar Corp. v. General Electric Co.*, 107 F.3d at 1549, 41 USPQ2d at 1805, emphasis added.

A description as filed is presumed to be adequate, unless or until sufficient evidence or reasoning to the contrary has been presented by the examiner to rebut the presumption. *See, e.g., In re Marzocchi*, 439 F.2d 220, 224, 169 USPQ 367, 370 (CCPA 1971); M.P.E.P. § 2163.04. The examiner bears the initial burden of establishing *prima facie* case of unpatentability by showing, by a preponderance of evidence, why a person skilled in the art

would not recognize in an applicant's disclosure a description of the invention defined by the claims. *In re Wertheim*, 541 F.2d 257, 263, 191 USPQ 90, 97 (CCPA 1976).

The Office Action gives no reasons why one of ordinary skill in the art would not be enabled to make and use the claimed invention based on Appellant's specification. (Office Action, pp. 3-4.) The Examiner, therefore, has not fulfilled the Office's burden of established a *prima facie* case that the specification fails to satisfy the requirements of 35 U.S.C. § 112, first paragraph. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

In particular, the Examiner asserts, "Since the section that Appellant referred as Description of the Invention is an exact duplicate of the independent and dependent original claims listed from page 12 to 16, Examiner considers the disclosure of the invention as having only two parts: BACKGROUND OF THE INVENTION and CLAIMS." (Office Action, p. 8.) Appellant disagrees. The "Description of the Invention" section is not an "exact duplicate" of the claims, as asserted by the Examiner. (*Id.*) For example, page 10, line 26 to page 11, line 25 describe exemplary embodiments encompassed by the invention recited in the listing provided in the "Claims" section. Moreover, the repetition of claim language in the specification is no reason to interpret the "Description of the Invention" section to be claims or background; and the assertion does not support a rationale for lack of enablement. Accordingly, the rejection of claims 1-20 under Section 112, first paragraph is improper and Appellant respectfully requests that this rejection be withdrawn.

Furthermore, Appellant submits claims 1-20 satisfy the requirements of 35 U.S.C. § 112, first paragraph. As described in the "Background" section of Appellant's disclosure, one of ordinary skill in the art of secure electronic transactions would be familiar with, for instance, enciphering and/or signing algorithms using asymmetric keys (e.g., private key, public key), public key infrastructures (PKI), and the X509 format. (*See, e.g.,* Specification,

pp. 1:13-6:13.) Appellant respectfully submits one of ordinary skill in the art would have sufficient knowledge to make and use the claimed invention based on the "Detailed Description" section between page 6, line 14 and page 11, line 25 of Appellant's specification. Accordingly, claims 1-20 are enabled by the specification. Appellant, therefore, respectfully requests that the Examiner's rejection of claims 1-20 under 35 U.S.C. § 112, first paragraph be withdrawn for this reason as well.

Rejection of Claims 1-9 and 13-20 Under 35 U.S.C. § 102(e)

Appellant traverses the rejection of claims 1-9 and 13-20 under Section 102(e) as allegedly being anticipated by U.S. Patent Application Publication No. 2003/0115457 to *Wildish et al.* ("*Wildish*"). In order to properly anticipate Appellant's claims under Section 102(e), each and every element of the claim in issue must be found, either expressly described or under the principles of inherency, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) The identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Further, the elements must be arranged as required by the claim. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

Claim 1: *Wildish* cannot support a rejection of claim 1 under Section 102(e) because the document fails to teach, at least, "digital data comprising data identifying at least one of: means of generating the private key, means of storing the private key on a medium, and means of signing with the private key."

Wildish discloses a method for relating a public key to a string of identifiers included in a digital certificate. The method enables an entity to construct a certificate chain leading from a root certificate authority to an end-entity. According to *Wildish*, a certificate server

16 includes a key pair generator 27 and a data storage device 28. (*Id at* ¶ 032.) Data storage device 28 stores digital certificates issued by certificate server 16. (*Id at* ¶ 032; FIG. 5.) These digital certificates include concatenated fields (ID1, ID2, ID3) having pseudonymic digital identifiers of certified entities 14, 16. (*Id at* ¶ 033; FIG. 5.)

The Examiner apparently asserts that *Wildish's* pseudonymic digital identifiers in concatenated fields (ID1, ID2, ID3) correspond to Appellant's claimed "digital data *identifying the proprietor* of said public key." (Office Action, p. 9.) In addition, it appears the Examiner asserts that key pair generator 27, data storage device 28, or CPU 20 corresponds to Appellant's claimed "digital data identifying ... means of generating the private key" and "digital data ... identifying ... means of signing with the private key," respectively. (*Id.*) On the contrary, *Wildish* says nothing with regard to the claimed "means of generating" and "means of signing."

As noted above, *Wildish's* pseudonymic digital identifiers merely identify an entity that produced a respective certificate (*Id.* at ¶¶ 0019, 033; FIG. 5.) For instance, the document states, "The pseudonyms ... could be chosen or generated by the root CA, or could be chosen or generated by some other entity. The generated pseudonyms may be in the form of random strings. Alternately, the pseudonym ... may be based, at least in part, on identity, or other information, contained in the certificate." (*Id.*) The *identity* of an entity cannot be considered to correspond to "*means* of generating the private key" and "*means* of signing with the private key," as recited in claim 1. (Emphasis added.) Moreover, *Wildish's* digital certificates do not include any data *identifying* key pair generator 27, data storage device 28 and CPU 20 in the concatenated fields. As such, neither these components nor their identities can be considered to correspond to "digital data comprising data identifying at least one of:

means of generating the private key, means of storing the private key on a medium, and means of signing with the private key," as recited in claim 1.

Furthermore, the Examiner has already asserted that the pseudonymic digital identifiers correspond to the "digital data identifying the proprietor." (Office Action, p. 9.) As such, these pseudonymic digital identifiers *cannot also* be considered to correspond to the claimed "digital data identifying ... means of generating the private key" and "digital data ... identifying ... means of signing with the private key."

Because *Wildish* does not disclose the above-identified features of claim 1, *Wildish* cannot support a rejection of claim 1 under 35 U.S.C. § 102(e). Appellant, therefore, respectfully requests that the rejection of claim 1 under be withdrawn.

Claim 8: Claim 8 although of different scope than claim 1, recites features similar to those in claim 1. Accordingly, claim 8 is allowable for the same reasons set forth above with regard to claim 1.

Claims 2-7, 9 and 13-20: Claims 2-7, 9 and 13-20 depend from claims 1 and 8. Thus, claims 2-7, 9 and 13-20 are allowable at least to their corresponding dependence from allowable claims 1 and 8.

Rejection of Claims 10-12 Under 35 U.S.C. § 103(a)

Appellant traverses the rejection of claim 10-12 under 35 U.S.C. § 103(a) as allegedly not being patentable over *Wildish* in view of U.S. Patent Application Publication No. 2004/0123107 to *Miyazaki et al.* ("*Miyazaki*"). Claims 10-12 depend from claim 8 and therefore include all the limitations of claim 8. Thus, *Wildish* fails to disclose or suggest the "digital data" identifying "means of generating" and "means of signing" of claims 10-12.

The Examiner relies on *Miyazaki* for its alleged disclosure of a message being accepted based on the probability of a key being used by a legitimate provider. (Office

Action, p. 7.) *Miyazaki* does not disclose the "digital data" missing from *Wildish* and the Examiner does not assert that *Miyazaki* makes any such disclosure. Accordingly, *Wildish* and *Miyazaki*, taken individually or in combination, do not disclose or suggest the subject matter recited in claims 10-12. Appellant, therefore, respectfully requests that the rejection of claims 10-12 under Section 103 be withdrawn.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

None.

X. Related Proceedings Appendix

None.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date February 26, 2009

By: /Steven Ashburn/
Steven Ashburn
Registration No. 56,636

VIII. CLAIMS APPENDIX

Claims involved in the appeal of U.S. Patent Application Serial No. 10/590,214:

1. (Previously presented) A method of producing a digital certificate in which a certification authority performs the steps of:

grouping together, in a data set, a public key and digital data comprising data identifying the proprietor of said public key and of an associated private key;

signing the data set in order to produce a digital certificate; and

storing the signed data set in a computer-readable storage medium,

wherein the digital data also comprise data identifying at least one of: means of generating the private key, means of storing the private key on a medium, and means of signing with the private key.

2. (Previously presented) A method according to claim 1, in which the data identifying the means of generating the private key comprise data identifying:

- a method of generating the private key, and/or
- hardware on which the method of generating the private key is implemented, and/or
- a place on which the method of generating the private key is implemented.

3. (Previously presented) A method according to claim 1, in which the data identifying the means of storing the private key comprise data identifying:

- a method of storing the private key on a medium, and/or

- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored.

4. (Previously presented) A method according to claim 1, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

5. (Previously presented) A method according to claim 2, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

6. (Previously presented) A method according to claim 2, in which the data identifying a method comprise:

- a reference identifying said method of generating the private key, and/or
- an identification of an inventor of said method of generating the private key, and/or
- an indication of a security level of said method of generating the private key according to ISO 15408.

7. (Previously presented) A method according to claim 2, in which the data identifying a place comprise:

- an identification of said place, and/or
- an identification of a security level of said place according to ISO 15408.

8. (Previously presented) A digital certificate stored in a computer-readable medium, comprising:

- a public key;
- data identifying a proprietor of the public key and of an associated private key; and
- data identifying at least one of means of generating the private key, means of storing the private key on a medium, and means of signature with said private key.

9. (Original) A certificate according to claim 8, of the X509 type according to a standard Information Technology – Open Systems Interconnection – The Directory : Public Key and Attribute Certificate Frameworks, dated March 2000, of the International Telecommunication Union, in which a set of predefined free fields are used to store the digital data identifying:

- a method of generating the private key, and/or
- hardware on which the method of generating the private key is implemented, and/or
- a place on which the method of generating the private key is implemented, and/or
- a method of storing the private key on a medium, and/or

- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored, and/or
- a signature method using the private key, and/or
- a storage medium on which the said signature method is stored.

10. (Previously presented) A method of using a digital certificate according to claim 8, comprising the following steps:

- receiving a message signed with a private key,
- reading, in the digital certificate, data identifying means of generating the private key and/or means of storing the private key on a medium and/or means of signing with the private key,
- deducing therefrom a probability of said private key having been used by a legitimate proprietor of said private key,
- according to said probability, accepting or refusing the electronic message.

11. (Original) A method according to claim 10, in which the message is accepted solely if the probability of the said key having been used by its legitimate proprietor is greater than a predefined value.

12. (Original) A method according to claim 10, in which:

- the message is accepted if the probability is greater than a first value (VB1),
- a confirmation of the said message is requested if the probability is between the first value (VB1) and a second value (VB2) less than the first value, and

- the message is refused if the probability is less than the second value (VB2).

13. (Previously presented) A method according to claim 2, in which the data identifying the means of storing the private key comprise data identifying:

- a method of storing the private key on a medium, and/or
- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored.

14. (Previously presented) A method according to claim 2, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

15. (Previously presented) A method according to claim 3, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

16. (Previously presented) A method according to claim 3, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or

- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

17. (Previously presented) A method according to claim 13, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

18. (Previously presented) A method according to claim 3, in which the data identifying a method comprise:

- a reference identifying said method of storing the private key, and/or
- an identification of an inventor of said method of storing the private key, and/or
- an indication of a security level of said method of storing the private key according to ISO 15408.

19. (Previously presented) A method according to claim 4, in which the data identifying a method comprise:

- a reference identifying said method using the private key, and/or
- an identification of an inventor of said method using the private key, and/or

- an indication of a security level of said method using the private key according to ISO 15408.

20. (Previously presented) A method according to claim 5, in which the data identifying a method comprise:

- a reference identifying said method, and/or
- an identification of an inventor of said method, and/or
- an indication of a security level of said method according to ISO 15408.

IX. EVIDENCE APPENDIX

None

X. RELATED PROCEEDINGS APPENDIX

None